The President's National Security Telecommunications Advisory Committee

A Model of Industry and Government Partnership

Mr. Guy Copeland
Computer Sciences Corporation
3170 Fairview Park Drive, Falls Church, VA 22042
Tel: 703-641-2561 Fax: 703-849-1005
EMail: gcopelan@csc.com
NSTAC Info: http://www.ncs.gov/nstac.htm
NSTAC Secretariat: 703-607-6209

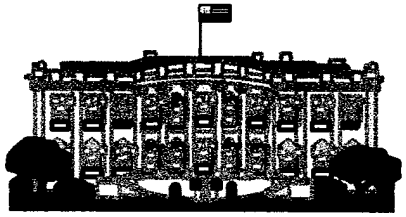
Agenda

- NSTAC Background
- Critical Infrastructure Risk Assessments
  - Telecommunication
  - Electric Power
  - Financial Services
  - Transportation
- National Coordinating Mechanism
- Questions

NSTAC Formation

- Established: President Ronald Reagan, Executive Order 12382, September 1982, as amended
- Authority: Federal Advisory Committee Act
- Executive Agent: William Cohen, Secretary of Defense
  - Designated Federal Official: LTG David Kelley, Manager, National Communications System (NCS) & Director, Defense Information Systems Agency (DISA)
  - Up to 30 CEOs Telecommunications and Information Industries
- Chair: Currently Mr. Charles R. Lee, GTE
- Vice Chair: Currently, Mr. Van B. Honeycutt, CSC.

Joint Government/Industry Partnership



Executive Office of the President
NSC, OMB, OSTP,
Executive Agent, DFO, NCS

National Security Telecommunications Advisory Committee
30 Senior Executives

NS/EP Telecommunications and Information Systems

15 Years of NSTAC Results

- National Coordinating Center (NCC) for Telecommunications
- International Diplomatic Telecommunications
- Electromagnetic Pulse (EMP) Assessment
- Commercial Network Survivability (CNS) Assessment
- Telecommunications Industry Mobilization (TIM) Assessment
- Commercial Satellite Survivability (CSS) Assessment
- Telecommunications Service Priority (TSP)
- Network Security Information Exchange (NSIE)
- Enhanced Call Completion (ECC)
- Cellular Priority Access Service (CPAS)
- Government Emergency Telecommunications Service (GETS).

National Coordinating Center for Telecommunications (NCC)

- Established 1984
- Industry members: AT&T, COMSAT, GTE, ITT, MCI, NTA, Sprint, Worldcom, USTA
- Government members:
  - Departments of Defense, Energy, Justice and State
  - Agencies: FCC, FEMA, GSA
- Assists in initiation, coordination, restoration and reconstitution of NS/EP telecommunications services or facilities (under all conditions, crises, or emergencies)
- Exercises, response planning, training
- Examining expanded future role (I&W, NCM)
- Successful model for daily industry/government partnership

Network Security Information Exchange

- Growing Vulnerability of the Public Switched Network, NRC, 1989

  "...NCS should consider how to protect the public networks from penetration by hostile users..."

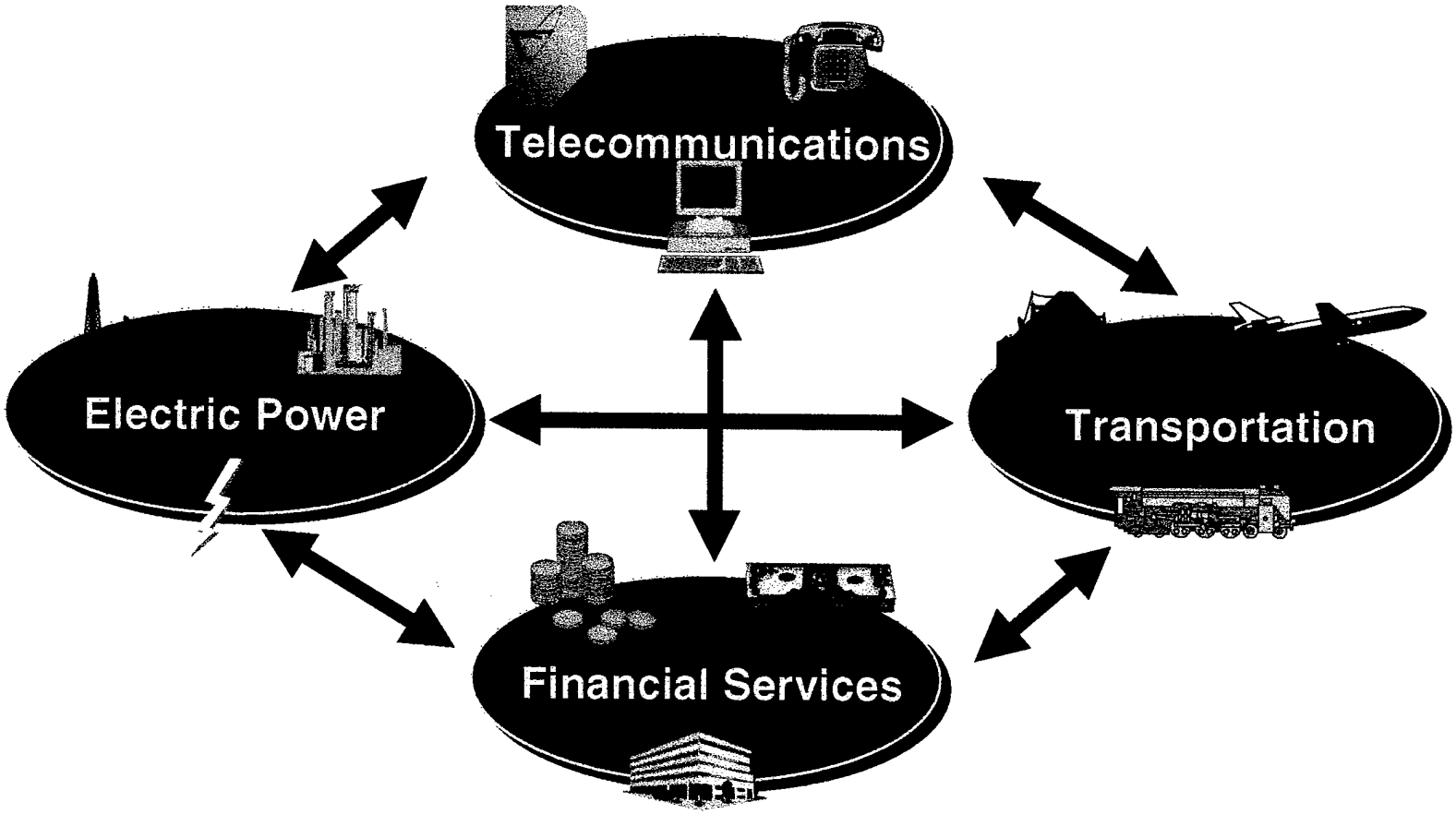
- April 1990, NSC memo to Manager, NCS

  ... the 'hacker' threat."

- Our opponents were sharing information, why not us?
- Based on Bellcore's Security Information Exchange
- First meeting June 1991; 40th meeting March 1998
- Members 1991: 9 Government; 9 NSTAC
- Members 1998: 10 Government; 20 NSTAC

Critical Infrastructure Risk Assessments

Critical Infrastructure Interdependence



Telecommunications Risk Assessment

Telecommunications Risk Assessment

- **"An Assessment of the Risk to the Security of Public Networks"**
- **Prepared jointly by Government and Industry Network Security Information Exchanges**
- **NSIE's update periodically**
- **Available through the Office of the Manager, National Communications System**

Telecommunications - Conclusions

- Overall risk to the public network is greater than reported in the 1993 risk assessment
- Reliance on the public network is growing
- Complexity of the network (technology, interfaces, size, etc.) is growing
- Threats are outpacing deterrents
- Vulnerabilities are outpacing the implementation of protective measures

Telecom Industry's Top Security Concerns

- Increased number of access points and networking
- Collocation of carriers into one carrier's infrastructure basket(s)
- Increased number of interconnected inexperienced systems administrators and processes
- Embedded Operations Channels of PTN Signaling and Transport Protocols (e.g., SONET DCC, ATM OAM Cells, SS7 Network Management Messages) gives virtually unlimited access to everything and everyone connected (networked) to them
- Internet and Intranet Exploitable technology used for access to Network Operations and Signaling Systems
- Local Number Portability Added complexity, dependencies and single points of failure
- Lack of Fidelity Bonds, Criminal Background Checks
- CALEA Control Requirements of Section 229 of the Act

Network Reliability and Interoperability Council, 4/97

Public Switched Network Security

"Within the PSN, intruders have already compromised nearly all categories of activities, from switching systems to operations, administration, maintenance, and provisioning (OAM&P) systems, and to packet data networks. Private branch exchanges (PBXs) and corporate networks that tie into the public network have crashed or disrupted signal transfer points (STPs), traffic switches, OAM&P systems, and other network elements. They have planted destructive 'time bomb' programs designed to shut down switching hubs, disrupted E-911 services throughout the eastern seaboard, and boasted that they have the capability to bring down all switches in Manhattan."

Reliability and Vulnerability Working Group, IITF

Electric Power Risk Assessment

Electric Power - Key industry trends

- Shift from:
  - Proprietary control protocols to Utility Control Architecture
  - Mainframe applications to client-server
  - Isolated control centers to interconnections
  - Manual on-site maintenance to remote substation automation
- FERC rulemaking on open access to transmission system information (OASIS):
  - Forcing utilities to separate transmission control from power marketing
  - Utilities will post transmission system information on Internet web hosts
- Deregulation will lead to major industry restructuring
- Increased competition inhibits information sharing

Electric Power - Observations

- **Control centers and control center computers today are relatively isolated from public networks**
  - **Use of private networks for transport**
  - **Limited or no connectivity with corporate networks**
  - **Multiple operational checks within control applications**
  - **Remote maintenance access by EMS vendors is the primary vulnerability**

Electric Power - Observations (2)

- **Substation automation is source of most exposure**
  - **Maintenance/administration ports on:**
    - **Remote Terminal Units (RTU's)**
    - **Protective relays**
    - **Circuit breakers**
  - **Widespread reliance on dial-up access**
  - **Rudimentary access controls**
  - **Combined with simple critical node analysis, could allow simple attack to cause major network outage**

Electric Power - Information security

- Information security awareness just beginning to mature
  - Proliferation of modems on network-attached PCs
  - Simple dial-back access controls on modem pools
  - Virus response programs
  - Limited network password/ID management
  - Less than half the companies interviewed have a focal point for information security
- Physical threats (weather, natural disasters, vandalism) far outweigh network-based threats
- Consistent interest in:
  - Mechanism for incident/vulnerability/threat information exchange
  - Providing threat awareness briefing to senior managers

Financial Services Risk Assessment

Financial Services Objectives

- **Assess the security and robustness of the financial services infrastructure at the national level relative to the identified threats to its networks and information systems**
- **Determine the risks to the financial services industry that derive from its dependence on information technology and the telecommunications infrastructure**
- **Examine the implications of trends regarding the industry's use of information systems and networks.**

Conclusions

- Perceptions vs. reality
  - Citibank was NOT a hack
  - Hackers/experts perpetuate
  - *Debt of Honor*, Tom Clancy
- Natural disasters and physical attacks
  - Few single points of failure
  - Considerable experience
- Cyber Risks
  - Year 2000 biggest challenge
- Cyber Threats
  - Reluctance to share (on all sides)

Findings

- U.S. financial services infrastructure is well protected to withstand all but a full-scale, national-level attack
- Security is fundamental consideration
  - Accountability and oversight to the board level
  - Integral element of risk management
  - Major investments: security, diversity, backup, recovery
- Government needs to provide more threat information
- Consideration should be given to the monitoring of emerging electronic payment systems
- There is an issue on adequate background checks at hire.

Transportation Risk Assessment

Transportation

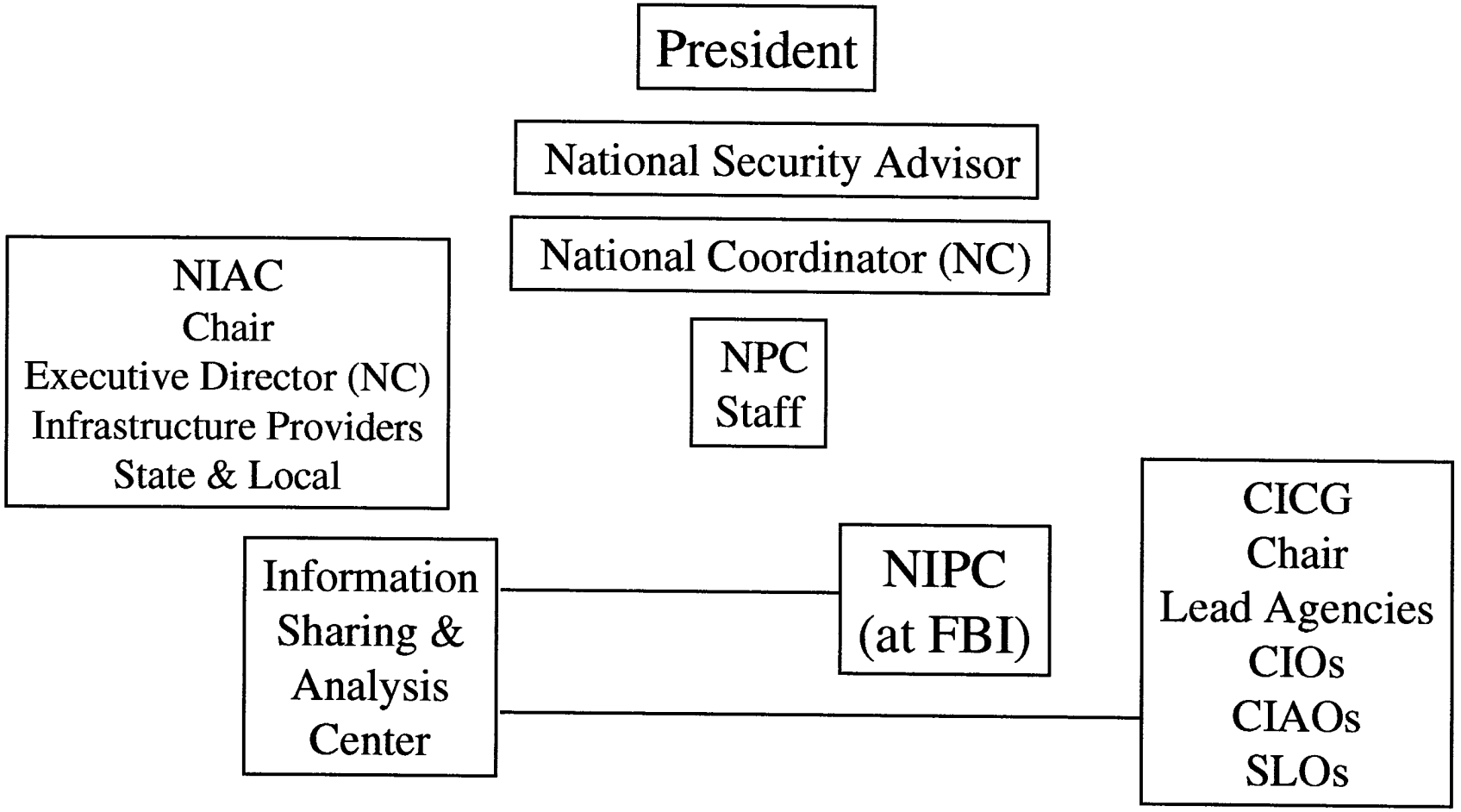
- Key elements of transportation infrastructure:
  - Air traffic control and airspace safety
  - Highway
  - Maritime
  - Rail
  - Trucking
  - Oil and natural gas pipelines
- Initial Workshop in Atlanta, September 10, 1997
- Interim report to NSTAC XX, December 11, 1997
- Continuing

Aside on Contacts with Industry

- Views on government involvement vary among individual industries, based on:
  - Existing information sharing and coordination mechanisms
  - Extent of regulatory controls
  - Experiences from other encounters

- However, industry is consistent in some views:
  - Suspicion of motivations for government involvement
  - Skepticism about threats
  - Concern about privacy and trust in any information exchange

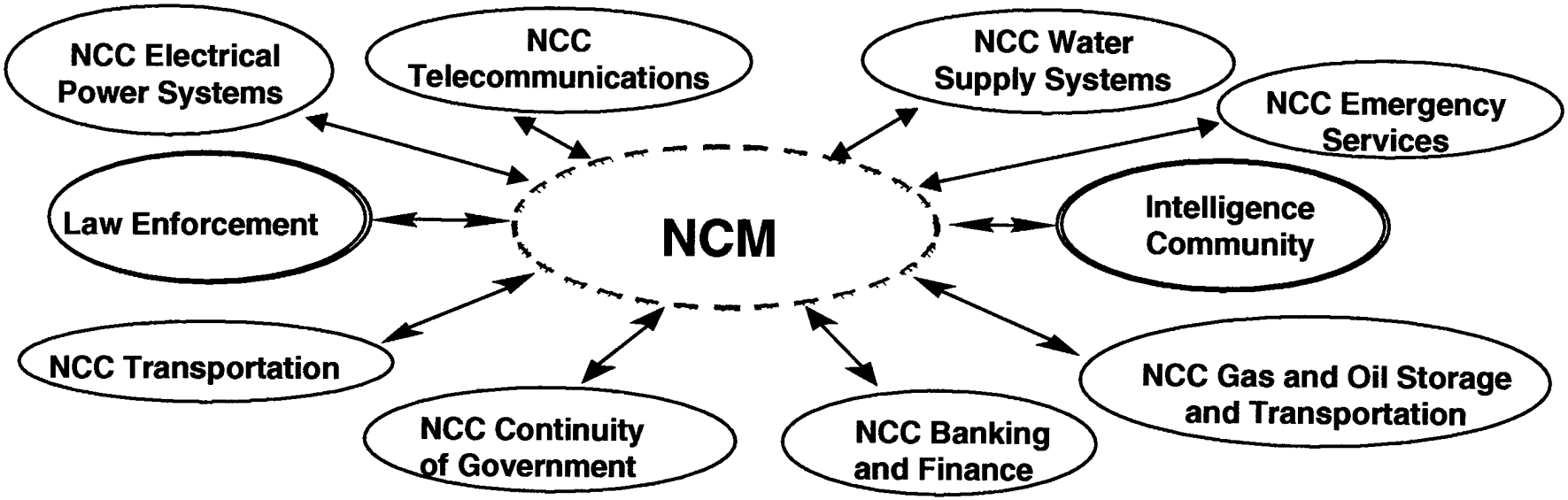
PDD-63, May 22, 1998



National Coordinating Mechanism (NCM)

National Coordinating Mechanism

The feasibility of the NCM depends on industry and Government's willingness to participate in the information-sharing process.



Reports

Many final reports can be found at:

http://www.ncs.gov/nstac/reports.html

Or by calling OMNCS at 703-607-6209

- **Electric Power Risk Assessment Report**
- **Issue Review - December 1997**
- **Intrusion Detection Subgroup Report**
- **Information Infrastructure Group Report**
- **Financial Services Risk Assessment Report**
- **Legislative and Regulatory Group Report**
- **Operations Support Group Report.**


NATIONAL SECURITY TELECOMMUNICATIONS
NSTAC
ADVISORY COMMITTEE

Questions?